UNITED STATES ATTORNEY'S OFFICE
Southern District of New York

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE
Friday, October 31, 2014
http://www.justice.gov/usao/nys

CONTACT: James Margolin, Jerika Richardson, Jennifer Queliz, Betsy Feuerstein
(212) 637-2600

DEFENDANT CHARGED IN MASSIVE INTERNET FRAUD SCHEME THAT INFECTED MILLIONS OF COMPUTERS WORLDWIDE EXTRADITED FROM ESTONIA TO THE SOUTHERN DISTRICT OF NEW YORK

Preet Bharara, the United States Attorney for the Southern District of New York, announced today the extradition of VLADIMIR TSASTSIN from Estonia to face charges of computer intrusion, wire fraud, and money laundering, among other offenses. The charges relate to the alleged operation of a massive and sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries. The malware secretly altered the settings on infected computers, enabling TSASTSIN and the six other charged defendants –Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, Konstantin Poltev, Andrey Taame, and Anton Ivanov – to digitally hijack Internet searches and re-route computers to certain websites and advertisements. TSASTSIN, an Estonian citizen, was arrested in Estonia on November 8, 2011, when the Indictment against him was unsealed. He arrived in the Southern District of New York yesterday, and was presented today before U.S. Magistrate Judge Gabriel W. Gorenstein.

Manhattan U.S. Attorney Preet Bharara said: "Now that Vladimir Tsastsin has been delivered to the Southern District of New York, he can answer for his alleged role in a scheme in which he and others manipulated Internet advertising techniques and reaped at least $14 million in ill-gotten gains in the process."

The following allegations are based on the Indictment and other court documents previously filed in Manhattan federal court:

From 2007 until October 2011, TSASTSIN, Gerassimenko, Jegorov, Aleksejev, Poltev, Taame, and Ivanov controlled and operated various companies that masqueraded as legitimate publisher networks (the "Publisher Networks") in the Internet advertising industry. The Publisher Networks entered into agreements with ad brokers under which they were paid based on the number of times that Internet users clicked on the links for certain websites or advertisements, or based on the number of times that certain advertisements were displayed on certain websites. Thus, the more traffic that went to the advertisers' websites and display ads, the more money the defendants earned under their agreements with the ad brokers. The

defendants fraudulently increased the traffic to the websites and advertisements that would earn them money and made it appear to advertisers that the Internet traffic came from legitimate clicks and ad displays on the defendants' Publisher Networks when, in actuality, it had not.

To carry out the scheme, the defendants and their co-conspirators used what are known as "rogue" Domain Name System ("DNS") servers, and malware ("the Malware") that was designed to alter the DNS server settings on infected computers. Victims' computers became infected with the Malware when they visited certain websites or downloaded certain software to view videos online. The Malware altered the DNS server settings on victims' computers to route the infected computers to rogue DNS servers controlled and operated by the defendants and their co-conspirators. The re-routing took two forms that are described in detail below: "click hijacking" and "advertising replacement fraud." The Malware also prevented the infected computers from receiving anti-virus software updates or operating system updates that otherwise might have detected the Malware and stopped it. In addition, the infected computers were also left vulnerable to infections by other viruses.

Click Hijacking

When the user of an infected computer clicked on a search result link displayed through a search engine query, the Malware caused the computer to be re-routed to a different website. Instead of being brought to the website to which the user asked to go, the user was brought to a website designated by the defendants. Each "click" triggered payment to the defendants under their advertising agreements. This click hijacking occurred for clicks on unpaid links that appeared in response to a user's query as well as clicks on "sponsored" links or advertisements that appeared in response to a user's query – often at the top of, or to the right of, the search results – thus causing the search engines to lose money. For example, when the user of an infected computer clicked on the domain name link for the official website of Apple-iTunes, the user was instead taken to a website for a business unaffiliated with Apple Inc. that purported to sell Apple software.

Advertising Replacement Fraud

Using the DNS Changer Malware and rogue DNS servers, the defendants also replaced legitimate advertisements on websites with substituted advertisements that triggered payments to the defendants. For example, when the user of an infected computer visited the home page of the Wall Street Journal, a featured advertisement for the American Express "Plum Card" had been fraudulently replaced with an ad for "Fashion Girl LA."

The defendants earned millions of dollars under their advertising agreements, not by legitimately displaying advertisements through their Publisher Networks, but rather by using the Malware to fraudulently drive Internet traffic to the websites and ads that would earn them more money. As a result, the defendants and their co-conspirators earned at least $14 million in ill-gotten gains through click hijacking and advertisement replacement fraud. The defendants laundered the proceeds of the scheme through numerous companies including, among others, Rove Digital, an Estonian corporation, and others listed in the Indictment.

* * *

TSASTSIN, 34, of Estonia, is charged with one count of wire fraud conspiracy, which carries a maximum sentence of 30 years in prison; one count of wire fraud, which carries a maximum sentence of 30 years in prison; one count of computer intrusion conspiracy, which carries a maximum sentence of 10 years in prison; one count of computer intrusion furthering fraud, which carries a maximum sentence of five years in prison; one count of computer intrusion by transmitting information, which carries a maximum sentence of 10 years in prison; one count of money laundering, which carries a maximum sentence of 30 years in prison; and 21 counts of engaging in monetary transactions of value over $10,000 involving fraud proceeds, each of which carries a maximum sentence of 10 years in prison. The maximum potential sentence in this case is prescribed by Congress and is provided here for informational purposes only, as any sentencing of the defendant will be determined by a judge.

Estonian nationals Gerassimenko, Jegorov, Aleksejev, Poltev, and Ivanov were also arrested in November 2011, and were all previously extradited to the United States. The last defendant, Taame, who is a Russian national, remains at large. Aleksejev pleaded guilty to conspiracy to commit unauthorized computer intrusion and computer intrusion on February 1, 2013, and was sentenced to 48 months in prison. Ivanov pleaded guilty to all charges on February 21, 2013, and was sentenced to time served.

The case against TSASTSIN and the remaining co-defendants is pending before U.S. District Judge Lewis A. Kaplan. The next conference is scheduled for November 5, 2014 at 2:30 p.m.

Mr. Bharara praised the outstanding investigative work of the Federal Bureau of Investigation, National Aeronautics and Space Administration-Office of the Inspector General, and the Estonian National Police and Border Guard Board. He also thanked the Office of International Affairs in the U.S. Department of Justice's Criminal Division for its assistance with the extradition.

This case is being handled by the Office's Complex Frauds and Cybercrime Unit. Assistant U.S. Attorneys Sarah Lai and Alexander Wilson are in charge of the prosecution.

The charges and allegations contained in the Indictment against TSASTSIN and the remaining defendants are merely accusations, and they are presumed innocent unless and until proven guilty.

14-318 ###